WE CLAIM:

1. A method for detecting impersonation based attacks at a wireless node of a wireless communication network, comprising the steps of:

a) providing an intrusion detection module with a copy of original data frames transmitted by the wireless node over a wireless interface;

b) detecting at the intrusion detection module incoming data frames received over the wireless interface; and

c) recognizing an impersonating attack when the information in the copy differs from the information in the incoming data frames.

2. The method of claim 1, wherein step a) comprises transmitting the copy over a secure link established between the wireless node and the intrusion detection module.

3. The method of claim 1, wherein the copy comprises only management frames.

4. The method of claim 1, wherein the copy includes a summary of the outgoing data frames.

5. The method of claim 4, wherein the summary of the outgoing data frames comprises frames that allow statistical comparisons.

6. The method of claim 4, wherein the summary comprises the number of the outgoing data frames transmitted over a time interval.

7. The method of claim 4, wherein the summary comprises the types of the original data frames.

8. The method of claim 1, wherein step b) comprises monitoring all wireless channels allocated to the wireless node and extracting the incoming data frames received over all the wireless channels.

9. The method of claim 1, wherein step c) comprises:

correlating the original data frames with the incoming data frames for detecting an inconsistency between the frames; and

upon detection of the inconsistency, further processing the received data frames for qualifying the impersonating attack.

10. An impersonation detection system for a wireless node of a wireless communication network, the node for transmitting original data frames over a wireless interface comprising:

an intrusion detection module for correlating the original data frames with incoming data frames received over the air interface; and

connection means between the wireless node and the intrusion detection module for providing the intrusion detection module with a copy of the original data frames.

11. The impersonation detection system of claim 10, wherein the intrusion detection module comprises:

a first receiving unit for receiving the copy;

an antenna for capturing the incoming traffic received on all transmission channels allocated to the wireless node;

a second receiving unit for detecting the incoming data frames from the incoming traffic; and

a data processing unit for correlating the copy with the incoming data frames and generating a impersonation detection signal.

12. The impersonation detection system of claim 11, wherein the intrusion detection module further comprises means for qualifying an intrusion attack based on the impersonation detected signal.

13. The impersonation detection system of claim 10, wherein the connection means comprises, when the intrusion detection module resides away from the wireless node:

a transmitting unit on the wireless node, for transmitting the copy to the intrusion detection module;

a secure link for connecting the wireless node with the intrusion detection module; and

a receiving unit on the intrusion detection module for receiving the copy.

14. The impersonation detection system of claim 12 wherein the secure link operates according to a communication protocol.

15. The impersonation detection system of claim 10, wherein the wireless network operates according to any wireless network technology.

16. The impersonation detection system of claim 10, wherein the secure link is established as inter-processes communication, when the intrusion detection module is integrated within the wireless node.

17. A wireless node for a wireless network comprising:

means for transmitting outgoing data frames over a wireless interface;

an intrusion detection module for correlating the outgoing data frames with incoming data frames received from the air interface; and

a secure link between the wireless node and the intrusion detection module for providing the intrusion detection module with a copy of the outgoing data frames.

18. The wireless node of claim 17, wherein the intrusion detection module comprises:

a first receiving unit for receiving the copy of the outgoing data frames;

an antenna for capturing the incoming traffic carried on all transmission channels allocated to the wireless node;

a second receiving unit for detecting the incoming data frames from the incoming traffic; and

a data processing unit for correlating the copy of the outgoing data frames with the incoming data frames and generating an impersonation detected signal.

19. The an impersonation detection system of claim 18, wherein the intrusion detection module further comprises means for qualifying an intrusion attack based on the a impersonation detected signal.

20. The impersonation detection system of claim 18, wherein the wireless network operates according to any wireless network technology.